

CLAIMS**What is claimed is:**

- 1 1. A method in a data processing system for maintaining security during booting of the
2 data processing system, said method comprising:

3 during a boot process, interrogating a boot device for password information; and

4 in response to the boot device supplying password information corresponding to that
5 of a trusted boot device, booting the data processing system utilizing the boot device.

RPS920000109US1

1 2. The method according to Claim 1, wherein said password information includes at
2 least a serial number of the boot device.

1 3. The method according to Claim 1, wherein interrogating said boot device for
2 password information comprises startup software interrogating the boot device.

1 4. The method according to Claim 1, wherein interrogating said boot devices for
2 password information comprises interrogating a plurality of boot devices in sequence
3 according to a priority order until a boot device supplies password information corresponding
4 to that of a trusted boot device.

1 5. The method according to Claim 1, and further comprising:
2 storing a password in non-volatile storage of the data processing system; and
3 determining that said boot device has supplied password information corresponding
4 to a trusted boot device by hashing password information supplied by the boot device and
5 comparing the hashed password information with the stored password.

1 6. The method according to Claim 5, and further comprising obtaining said password
2 by interrogating the boot device for the password information with a password-protected
3 configuration routine.

- 1 7. A data processing system comprising:
- 2 a boot device;
- 3 a processor; and
- 4 memory coupled to said processor for communication, said memory including startup
- 5 software that, when executed by said processor during a boot process, interrogates the boot
- 6 device for password information and, responsive to the boot device supplying password
- 7 information corresponding to that of a trusted boot device, boots the data processing system
- 8 utilizing the boot device.

Approved for Release by NSA on 09-08-2013 pursuant to E.O. 13526

1 8. The data processing system of Claim 7, wherein said password information includes
2 at least a serial number of the boot device.

1 9. The data processing system of Claim 7, said data processing system having a plurality
2 of boot devices including the boot device, wherein said startup software interrogates said
3 plurality of boot devices for password information in sequence according to a priority order
4 until a boot device supplies password information corresponding to that of a trusted boot
5 device.

1 10. The data processing system of Claim 7, and further comprising non-volatile storage
2 that stores a password, wherein said startup software determines that said boot device has
3 supplied password information corresponding to a trusted boot device by hashing password
4 information supplied by the boot device and comparing the hashed password information
5 with the password stored in non-volatile storage.

1 11. The data processing system of Claim 10, said startup software including a password-
2 protected configuration routine that obtains said password by interrogating the boot device
3 for the password information.

09047086-0304
FOIA b 7 - D

12. A program product comprising:

a computer usable medium; and

startup software encoded within said computer usable medium, wherein said startup software causes a data processing system to interrogate the boot device for password information during a boot process and, responsive to the boot device supplying password information corresponding to that of a trusted boot device, to boot the data processing system utilizing the boot device.

1 13. The program product of Claim 12, wherein said password information includes at
2 least a serial number of the boot device.

1 14. The program product of Claim 12, said data processing system having a plurality of
2 boot devices including the boot device, wherein said startup software causes the data
3 processing system to interrogate said plurality of boot devices for password information in
4 sequence according to a priority order until a boot device supplies password information
5 corresponding to that of a trusted boot device.

1 15. The program product of Claim 12, wherein said startup software determines that said
2 boot device has supplied password information corresponding to a trusted boot device by
3 hashing password information supplied by the boot device and comparing the hashed
4 password information with a password stored in non-volatile storage of the data processing
5 system.

1 16. The program product of Claim 15, said startup software including a password-
2 protected configuration routine that obtains said password by interrogating the boot device
3 for the password information.

For filing only